

Declassified in Part - Sanitized Copy Approved for
Release 2013/07/15 : 3LIP | 3/4/88
CIA-RDP90M00551R001901130003-3

LCS Registry
ROOM NO.

BUILDING

BW09

REMARKS:

Hold back copy.

STAT

FROM:

ROOM NO.

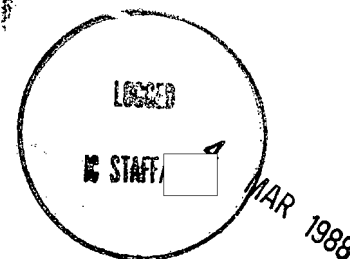
BUILDING

EXTENSION

Declassified in Part - Sanitized Copy Approved for
Release 2013/07/15 : ACES FORM 36-8
CIA-RDP90M00551R001901130003-3

LEG 6-SR

ICS 0790-88/1



MEMORANDUM FOR: Acting Director of Central Intelligence

FROM:

[Redacted]
Acting Director, Intelligence Community Staff

SUBJECT: Security Policies Controlling the Dissemination of
Controlled Information [Redacted]

REFERENCES:

- A. Memo from EXDIR/DIA to DD/CIA, 22 February 1988;
subject: Security Policies Governing the
Dissemination of Intelligence Information
(ER 88-0723X)
- B. DCID 1/7, effective 27 February 1987
- C. Memo from D/CCISCS/ICS to ADCI, 19 February 1987;
subject: Proposed Revision of DCID 1/7, "Security
Controls on the Dissemination of Intelligence
Information" (DCI/ICS-87-0785)
- D. Memo from ADCI to SCI Forum Members, 27 February 1987;
subject: DCID 1/7--Approval of Attached Revision
(DCI/ICS-87-0787)
- E. Memo from ADCI to NFIB Members, 27 February 1987;
subject: Revision of DCID 1/7, "Security Controls
on the Dissemination of Intelligence Information"
(DCI/ICS-87-0786)
- F. Memo from DIA to Chairman, SECOM, 13 June 1986;
subject: Revision of DCID 1/7 (U-6542/OS-4)
- G. Policy Statement on Procedures Governing Use of
DCID 1/7 Control Markings, June 1987 (OGC-87-51580)

25X1

25X1

25X1

25X1

1. References B. through E. (attached) document the chronology surrounding your approval of the revision of DCID 1/7 in February 1987. Accompanying your approval was the acknowledgment of a contentious portion of

~~SECRET~~

SUBJECT: Security Policies Controlling the Dissemination of
Controlled Information [redacted]

25X1

the DCID relating to the controls over NOCONTRACT restricted information. Your approval carried with it the direction that DIA and CIA work together toward accommodation of the differing views on rules governing the control of NOCONTRACT information. [redacted]

25X1

2. [redacted] reports a set of suggested changes to DCID 1/7 submitted by DIA in June 1986 (reference F.). The memorandum dissects different types of material and proposed use of such by categories of contractors supporting DIA and other government agencies. In brief, the memo contains the rationale for the recommendations and the mechanism for approval. The DIA recommendations were set aside at the December 1986 Forum meeting, when it was determined that the DIA proposal failed to include another category of "contractor." DIA then made the initial agreement to work the issue directly with CIA and permit the issuance of the language otherwise agreed upon in the DCID. It was stipulated that the DCI would be apprised of the contentious issue and the work in progress for a solution mutually acceptable to DIA and CIA. [redacted]

25X1

25X1

3. Reference G. (attached) is the policy statement produced by OGC that establishes procedures governing the use of controlled information. This was unanimously accepted and approved by DCI Security Forum members at a meeting in June 1987. DIA was represented at that meeting. At the time of approval, the Director of the Community Counterintelligence and Security Countermeasures Office (CCISCMO)/ICS reminded CIA and DIA of their obligation to resolve problems related to NOCONTRACT and ORCON controlled information. Then, in the July 1987 Forum meeting, DIA and CIA agreed to call together their respective data base technical and managerial personnel to attempt to resolve general and specific differences associated with NOCONTRACT controls. [redacted]

25X1

4. At the September 1987 Forum meeting, DIA went on record with the declaration that it had originally (December 1986) agreed to publishing a revision of DCID 1/7 with the understanding that DIA and CIA needed to reach agreement on certain NOCONTRACT issues. Further, DIA stipulated that depending on any agreement reached and terms of that agreement, it might request the Forum to consider a change to DCID 1/7. CIA officials report that their attempts to schedule meetings with DIA between July 1987 and the present were unsuccessful. DIA officials confirm that no meetings have taken place during this time. It appears clear that DIA's objections to the constraints imposed by the controls in DCID 1/7 have merit for negotiation. It is equally clear that DIA and CIA have not met in negotiation as instructed in your memo accompanying approval of the DCID. [redacted]

25X1

5. It is recommended that you assign CCISCMO the action in this matter to perform as the coordinating and motivating element between DIA and CIA. If any revisions to the DCID are warranted and agreed upon, CCISCMO is the office

SUBJECT: Security Policies Controlling the Dissemination of
Controlled Information [redacted]

25X1

to properly manage the administrative process via the DCI Security Forum and
get it into the approval channel through D/ICS to your office. A suggested
response to DIA is attached for your approval. [redacted]

25X1

[redacted]
Acting Director

25X1

Attachments:

1. References A. through G.
2. Proposed Response to DIA

SUBJECT: Security Policies Controlling the Dissemination of
Controlled Information

25X1

CCISCMO/ICS: (3 March 1988)

25X1

Distribution of ICS 0790-88/1:

Original - ADCI (w/atts)

1 - ER (w/atts)

1 - AD/ICS (w/atts)

1 - ICS Registry (w/atts)

1 - CCISCMO subject (DCID 1/7) (w/atts)

1 - CCISCMO chrono (wo/atts)

1 - chrono (w/atts)

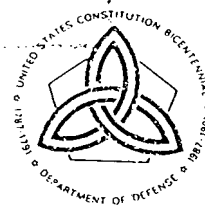
25X1



DEFENSE INTELLIGENCE AGENCY

WASHINGTON, D.C. 20340-1251

88-0723X



U-4392/OS-4

22 FEB 1988

MEMORANDUM FOR THE DEPUTY DIRECTOR, CENTRAL INTELLIGENCE AGENCY

SUBJECT: Security Policies Governing the Dissemination of Intelligence Information

Reference: DCI Directive 1/7, "Security Controls on the Dissemination of Intelligence Information," 27 February 1987.

1. The Department of Defense (DoD) relies heavily on contractors to develop large all-source data bases, sophisticated telecommunication systems, and state of the art ADP storage, data integration, retrieval, and computational capabilities. Strict compliance, however, with DCID 1/7 severely limits the development, maintenance, and use of these sophisticated systems, and Allied access to this critical data as well.
2. DCID 1/7 requires the consent of the "originator" for release of all material carrying the ORCON, NOCONTRACT, NOFORN, or PROPIN caveat. In large DoD intelligence data systems, the data bases have historically carried the caveats of the data being entered, even though there is no reference to source nor audit to a source on the data being entered. Subsequent effort, therefore, to identify the source of each data item to pursue "release authorization" has proven not only impractical, but also impossible in many circumstances. In June 1986, therefore, DIA proposed a specific change to the DCID 1/7 which recognized (1) the role of appropriately cleared contractors working under authorized government contract; (2) the fact that no source reference was made; and (3) would permit release of all-source data base information to those specific contractors. During discussions of that proposal, your staff raised the additional issue of DIA releasing data base information caveated NOFORN. To date, my staff has been unable to reach accord with your staff on these significant policy issues.
3. In addition to the difficulty in releasing automated data base information where there is no source attribution, there are also clear cases where contractor release is sought for data that does, in fact, clearly identify the source. In late 1985 this Agency sought authorization to release automated message traffic to contractors involved in the joint DIA/CIA SAFE program. In January 1986, the DCI Security Committee agreed to this access, but with the stipulation that government personnel be present at all times. This guidance has proven to be wasteful and impractical due to personnel constraints. DoD/DIA does not have sufficient resources to support major systems development or enhancement initiatives without reliance on contractors who possess the required security clearances.

ILLEGIB



4. In summary, strict compliance with the provisions of DCID 1/7 severely limits use of available technology to improve intelligence support to operational forces. I would appreciate your support in a joint effort to review the existing policy with the objective of establishing a new policy that adequately protects sensitive intelligence sources while authorizing Senior Officials of the Intelligence Community (SOICs) to make controlled and auditable release of NOFORN, NOCONTRACT, ORCON, and PROPIN intelligence information where sources are unidentified and unidentifiable. In the interim, request authority as the SOIC for DIA, to grant release of caveated intelligence in DIA data bases where the originator cannot be determined. Secondly, standard and practical procedures must be established for authorizing system development contractor access to source identified intelligence data where operationally required. In this regard, specifically request that DIA be relieved from the requirement that government personnel be present when SAFE contractors have access to NOCONTRACT and ORCON information.



Executive Director

STAT

ATTACHMENT B

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 1/7¹

SECURITY CONTROLS ON THE DISSEMINATION OF INTELLIGENCE INFORMATION

(Effective 27 February 1987)

Pursuant to the provisions of Section 102 of the National Security Act of 1947, Executive Order 12333, Executive Order 12356, and implementing directives thereto, policies, controls, and procedures for the dissemination and use of intelligence information and related materials are herewith established.

Part I

1. Purpose

This directive establishes policies, controls, and procedures for the dissemination and use of intelligence to ensure that, while facilitating its interchange for intelligence purposes, it will be adequately protected. This directive amplifies applicable portions of the 23 June 1982 Information Security Oversight Office (ISOO) Directive No. 1, which implements Executive Order 12356. Additional controls are established on the dissemination of intelligence to foreign governments and to foreign nationals and immigrant aliens, including those employed by the US Government. Policy and procedures governing the release of intelligence to contractors and consultants are set forth in part II of this directive.

2. Definitions

- a. Intelligence information and related materials (hereinafter referred to as intelligence) includes the following classified information:
 - foreign intelligence and counterintelligence as defined in Executive Order 12333;
 - information describing US foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodology used for the acquisition, processing, or exploitation of such intelligence; foreign military hardware obtained for exploitation; and photography or recordings resulting from US intelligence collection efforts; and
 - information on Intelligence Community protective security programs (e.g., personnel, physical, technical, and information security).
- b. "Need-to-know" is the determination by an authorized holder of classified information that access to specific intelligence in his/her possession is required by another person to perform a specific and authorized function to carry out a national security task. Such persons must possess an appropriate security clearance and access approvals.

3. General Applicability

- a. The controls and procedures established by this directive shall be applied uniformly in the dissemination and use of intelligence originated by all Intelligence Community components.

¹ This directive supersedes DCID 1/7, effective 7 January 1984.

FOR OFFICIAL USE ONLY

- b. The substance of this directive shall be promulgated by each Intelligence Community component, and appropriate procedures permitting prompt interagency consultation will be established and promulgated. To this end, each Intelligence Community component will designate a primary referent.

4. Use By and Dissemination Among US Intelligence Community Components

Executive Order 12356 provides that classified information originating in one US agency shall not be disseminated beyond any recipient agency without the consent of the originating agency. However, to facilitate use and dissemination of intelligence within and among Intelligence Community components and to provide for the provision of intelligence to consumers, the following controlled relief to the "third agency rule" is hereby established:

- Each Intelligence Community component consents to the use of its intelligence in intelligence products of other components and to the dissemination of those products within the Intelligence Community, except as specifically restricted by this directive.

5. Use By and Dissemination to US Components Outside the Intelligence Community

- a. Classified intelligence, even though it bears no restrictive control markings, will not be released in its original form to US components outside the Intelligence Community without the consent of the originator.
- b. Any component disseminating intelligence beyond the Intelligence Community assumes responsibility for ensuring that recipient organizations agree to observe the restrictions prescribed by this directive and to maintain adequate safeguards.

6. Dissemination to Foreign Nationals or Contractors

- a. Intelligence, even though it bears no restrictive control markings, will not be released to foreign nationals or immigrant aliens (including those employed by, used by, or integrated into the US Government) without the permission of the originator.
- b. Release of intelligence to a foreign contractor or company under contract to the US Government will be made according to the provisions of paragraph 7 below through the government under which the foreign contractor or company operates. Direct release from the US Government to a foreign company or contractor is prohibited.

7. Dissemination to Foreign Governments

- a. Intelligence, even though it bears no restrictive control markings, will not be released in its original form to foreign governments without the permission of the originator.
- b. Information contained in intelligence of another Intelligence Community component, which bears no restrictive control markings, may be used by recipient Intelligence Community components in reports provided to foreign governments provided that:
 - no reference is made to the source documents on which the released product is based;
 - the information is extracted or paraphrased to ensure that the source or manner of acquisition of the intelligence is not revealed and cannot be deduced in any manner;
 - foreign release is made through established foreign disclosure channels and procedures as set forth in DCID 5/6.
- c. RESTRICTED DATA and FORMERLY RESTRICTED DATA are prohibited from foreign dissemination under the provisions of Sections 123 and 144 of Public Law 585, Atomic Energy Act of 1954, as amended.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

DCID 1/7-3

8. Authorized Control Markings and Their Use

a. "WARNING NOTICE—INTELLIGENCE SOURCES OR METHODS INVOLVED" (WNINTEL)

- This marking is used to identify classified intelligence whose sensitivity requires constraints on its further dissemination and use. This marking may be used only on intelligence that identifies or would reasonably permit identification of an intelligence source or method that is susceptible to countermeasures that could nullify or reduce its effectiveness.
- Classified intelligence so marked shall not be disseminated in any manner outside authorized channels² without the permission of the originating agency and an assessment by the SOIC in the disseminating agency as to the potential risks to the national security and to the intelligence sources or methods involved. In making such assessment, consideration should be given to reducing the risk to the intelligence sources or methods that provided the intelligence by sanitizing or paraphrasing the information so as to permit its wider dissemination. To avoid confusion as to the extent of dissemination and use restrictions governing the information involved, this marking may not be used in conjunction with special access or sensitive compartmented information (SCI) controls. This marking may be abbreviated as "WNINTEL" or "WN."

b. "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR" (ORCON)

- This marking is used to enable continuing knowledge and supervision by the originator of the use made of intelligence. This marking may be used only on classified intelligence that clearly identifies or would reasonably permit ready identification of an intelligence source or method that is particularly susceptible to countermeasures that would nullify or measurably reduce its effectiveness. This marking may not be used when an item of information will reasonably be protected by use of any other markings specified herein, or by the application of the "need-to-know" principle and the safeguarding procedures of the security classification system.
- Information bearing this marking may not be disseminated beyond the headquarters elements³ of the recipient organizations and may not be incorporated in whole or in part into other briefings or used in taking investigative action, without the advance permission of, and under conditions specified by, the originator. As this is the most restrictive marking herein, agencies will establish procedures to ensure that it is only applied to particularly sensitive intelligence and that timely procedures are established to review requests for further dissemination of intelligence bearing this marking. This marking may be abbreviated as "ORCON" or "OC."

c. "NOT RELEASABLE TO CONTRACTORS/CONSULTANTS" (NOCONTRACT)

- This marking is used to identify classified intelligence that shall not be released to contractors or consultants (hereinafter "contractors") without the permission of the originating agency. This marking may be used only on intelligence that is

² Unless otherwise specified by the Director of Central Intelligence in consultation with the National Foreign Intelligence Board (NFIB) or as agreed to between originating and recipient agencies, authorized channels are the Intelligence Community, as defined in Executive Order 12333, and Intelligence Community contractors and consultants and officials of agencies represented on the NFIB as determined on a "need-to-know" basis by recipient SOICs.

³ At the discretion of the originator, the term "headquarters elements" may include specified subordinate intelligence-producing components.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

DCID 1/7-4

provided by a source on the express or implied condition that it not be made available to contractors; or that, if disclosed to a contractor, would actually or potentially give him/her a competitive advantage, which could reasonably be expected to cause a conflict of interest with his/her obligation to protect the information. These restrictions do not apply to consultants hired under Office of Personnel Management procedures, or comparable procedures derived from statutory authorities of department or agency heads, and who are considered to serve as extensions of their employing offices. This marking may be abbreviated as "NOCONTRACT" or "NC."

d. "CAUTION-PROPRIETARY INFORMATION INVOLVED" (PROPIN)

— This marking is used, with or without a security classification, to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a trade secret or proprietary data believed to have actual or potential value. Information bearing this marking shall not be disseminated in any form to an individual, organization, or foreign government that has any interests, actual or potential, in competition with the source of the information without the permission of the originator. This marking may be used in conjunction with the "NOCONTRACT" marking to preclude dissemination to any contractor. This marking may be abbreviated as "PROPIN" or "PR."

e. "NOT RELEASABLE TO FOREIGN NATIONALS" (NOFORN)

— This marking is used to identify classified intelligence that may not be released in any form to foreign governments, foreign nationals, or non-US citizens without permission of the originator. This marking may be used on intelligence that, if released to a foreign government or national(s), could jeopardize intelligence sources or methods, or when it would not be in the best interests of the United States to release the information from a policy standpoint upon specific determination by a SOIC. SOICs are responsible for developing, publishing, and maintaining guidelines consistent with the policy guidance herein for use in determining the foreign releasability of intelligence they collect or produce. These guidelines shall be used in assigning NOFORN control markings, and by primary referents (paragraph 3.b. above applies) in responding to inquiries from other organizations on application of this control. This marking may be abbreviated "NOFORN" or "NF."

f. "AUTHORIZED FOR RELEASE TO (name of country(ies)/international organization)" (REL)

— This marking is used to identify classified intelligence that an originator has predetermined to be releasable or has released, through established foreign disclosure procedures and channels, to the foreign country(ies)/international organization indicated. No other foreign dissemination of the material is authorized (in any form) without the permission of the originator. This marking may be abbreviated "REL (abbreviated name of country(ies)/international organization)." In the case of intelligence controlled under DCID 6/2, authorized distribution indicators, published separately, may be used instead of the "REL" control marking.

9. Procedures Governing Use of Control Markings

- a. Any recipient desiring to use intelligence in a manner contrary to the restrictions established by this directive shall obtain the advance permission of the originating agency. Such permission applies only to the specific purpose agreed to by the

FOR OFFICIAL USE ONLY

originator and does not automatically apply to all recipients. Originators will ensure that prompt consideration is given to recipients' requests with particular attention to reviewing and editing, if necessary, sanitized or paraphrased versions to derive a text suitable for release subject to lesser or no control markings.

- b. The control markings authorized above shall be shown on the title page, front cover, and other applicable pages of documents, incorporated in the text of electrical communications, shown on graphics, and associated (in full or abbreviated form) with data stored or processed in automated data processing systems. The control markings also shall be indicated by parenthetical use of the marking abbreviations at the beginning or end of the appropriate portions. If the control markings apply to several or all portions, the document may be marked with a statement to this effect rather than marking each portion individually.
- c. The control markings in paragraph 8 shall be individually assigned at the time of preparation of intelligence products and used in conjunction with security classifications and other markings specified by Executive Order 12356 and its implementing ISOO Directive. The markings shall be carried forward to any new format in which the same information is incorporated, including oral and visual presentations.

10. Obsolete Restrictions and Markings

The following markings are obsolete and will not be used subsequent to the date of this directive: WARNING NOTICE-SENSITIVE SOURCES AND METHODS INVOLVED, WARNING NOTICE-INTELLIGENCE SOURCES AND METHODS INVOLVED, WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED, CONTROLLED DISSEM, NSC PARTICIPATING AGENCIES ONLY, INTEL COMPONENTS ONLY, LIMITED, CONTINUED CONTROL, NO DISSEM ABROAD, BACKGROUND USE ONLY, NO FOREIGN DISSEM, USIB ONLY, and NFIB ONLY. Questions with respect to the current application of control markings authorized by earlier directives on the dissemination and control of intelligence and used on documents issued prior to the date of this directive should be referred to the originating agency or department.

11. Reporting Unauthorized Disclosures

Violations of the foregoing restrictions and control markings that result in unauthorized disclosure by one agency of the intelligence of another shall be reported to the Director of Central Intelligence through the Unauthorized Disclosure Analysis Center.

Part II

12. Policy and Procedures Governing the Release of Intelligence to Contractors and Consultants

- a. Intelligence Community components may release ⁴ selected intelligence ⁵ to contractors and consultants (hereinafter "contractors" ⁶) without referral to the originating components provided that:

⁴ Release is the authorized visual and/or physical disclosure of intelligence.

⁵ The term "selected intelligence" excludes Foreign Service reports, SCI, and material bearing ORCON, NOCONTRACT, or PROPIN control markings. Foreign Service reports may be released only with the permission of the Department of State. Release of intelligence material bearing ORCON, NOCONTRACT, or PROPIN markings is governed by paragraph 8 or this directive.

⁶ Non-Intelligence Community components of the executive branch of government under contract to fulfill an intelligence support role may be treated as members of the Intelligence Community. In that event, release will be made only with the consent of the originator, will be solely for the specific service required by the contract, and will not include authority to disseminate intelligence further. Government-owned, contractor-operated (GOCO) laboratories performing classified services in support of the intelligence mission of an Intelligence Community component, and which are designated as authorized channels by a SOIC or his/her designee, are not considered as contractors subject to the provisions of this directive.

FOR OFFICIAL USE ONLY

DCID 1/7-6

- (1) Release is made only to private individuals or organizations certified by the SOIC (or his/her designee) of the sponsoring organization as being under contract to the United States Government for the purpose of performing classified services in support of a national security mission; and as having a demonstrated "need-to-know" and an appropriate security clearance or access approval. If retention of intelligence by the contractor is required, the contractor must have an approved storage facility.
- (2) The SOIC of the sponsoring agency, or his/her designee, is responsible for ensuring that releases to contractors are made pursuant to this policy statement and through established channels.
- (3) The sponsoring agency maintains a record of material released.
- (4) Contractors maintain such records as will permit them to account for all intelligence received, disposed of or destroyed, and produced and held by them for the duration of the contract and permit identification of all persons who have had access to intelligence in their custody.
- (5) Contractors do not reproduce any intelligence without the permission of the sponsoring agency and classify, control, and account for reproduced copies in the same manner as for originals.
- (6) Contractors destroy intelligence only according to guidelines and by standards set by the sponsoring agency.
- (7) Contractors make provisions to ensure that intelligence in their custody is not released to foreign nationals, whether or not they are employees or contractors themselves, except with the permission of the originating agency through the sponsoring agency, and then released through established channels.
- (8) Contractors receiving intelligence do not release it: to any of their components or employees not directly engaged in providing services under the contract; or to any other contractor (including subcontractors), without the consent of the sponsoring agency (which shall verify that any second contractors satisfy all security requirements herein).
- (9) Any SCI released to contractors is controlled pursuant to the provisions of DCID 1/19, *Security Policy for Sensitive Compartmented Information*, effective 19 February 1987.
- (10) Contractors agree that all intelligence released to them, all reproductions thereof, and all other material they may generate based on or incorporating data therefrom (including authorized reproductions), remain the property of the US Government and will be returned upon request of the sponsoring agency or expiration of the contract, whichever comes first.
- (11) Sponsoring agencies arrange for, and contractors agree that, upon expiration of contracts, all released intelligence, all reproductions thereof, and all other materials based on or incorporating data therefrom, are returned to the sponsoring agency; or all or a specified part of such items are retained by the contractor under all applicable security and accountability controls when the contractor has a specific need for such retention that is validated by the sponsoring agency.
- (12) Sponsoring agencies delete: the CIA seal, the phrase "Directorate of Operations," the place acquired, the field number, the source description, and field dissemination from all CIA Directorate of Operations reports passed to contractors, unless prior approval to do otherwise is obtained from CIA.

FOR OFFICIAL USE ONLY

- b. National Intelligence Estimates (NIEs), Special National Intelligence Estimates (SNIEs), and Interagency Intelligence Memoranda will not be released to contractors. Such materials shall be marked NOT RELEASABLE TO CONTRACTORS/CONSULTANTS. However, information in them may be made available to contractors, without identification as national intelligence, by the SOIC of the agency authorizing its release.
- c. Intelligence which by reason of sensitivity of content bears control markings "CAUTION—PROPRIETARY INFORMATION INVOLVED," "NOT RELEASABLE TO CONTRACTORS/CONSULTANTS," or "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR," as specified in Part I of this directive, will not be released to contractors unless special permission has been obtained from the originator.
- d. Intelligence Community security policy requires that the government maintain control over sensitive intelligence and release to contractors only that information required to perform tasks beyond the capability of the government. The DCI has determined that there are significant risks to national security in contracting out support services or functions such as operation of telecommunications centers, automated data systems or other facilities when this permits broad contractor access to all-source or other sensitive intelligence information. Accordingly, Intelligence Community departments and agencies are cautioned fully to consider the consequences of contracting out these services pursuant to Office of Management and Budget Circular A-76, or similar guidance, in cases where the government's control of sensitive intelligence would be substantially diminished or where contractor access to such data would be unnecessarily expanded.

13. Interpretation

Questions concerning the implementation of this policy and these procedures shall be referred to the Community Counterintelligence and Security Countermeasures Staff/Intelligence Community Staff.

FOR OFFICIAL USE ONLY


~~SECRET~~ATTACHMENT DCI/ICS-87-0785
19 February 1987


25X1

25X1

MEMORANDUM FOR: Acting Director of Central Intelligence

VIA: Director, Intelligence Community Staff
Deputy Director, Intelligence Community StaffFROM: Director, Community Counterintelligence and Security
Countermeasures Staff, Intelligence Community StaffSUBJECT: Proposed Revision of DCID 1/7, "Security Controls on
the Dissemination of Intelligence Information"

1. Attached for your approval is the SCI Forum-proposed revision of DCID 1/7 which specifies the markings that can or must be placed on documents, or surrogates thereof, containing intelligence information; the rules governing when such markings can be used; and the rules for use of the marked documents. With the exception of one paragraph, discussed below, the draft is not contentious. The Community feels so strongly that a revised draft is needed that the military members of the Forum support reissuance despite their continuing dissatisfaction with the contentious paragraph. The attached copy of the existing version, with its indicated changes and the explanation of those changes, shows the limited nature of the revisions. 

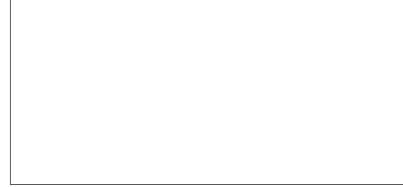
2. The contention involves paragraph 8c, which sets forth the restrictions in releasing intelligence information, identified by NOCONTRACT, to government contractors and consultants. The proposed revision carries forward the old rules unchanged but the DoD services and DIA oppose those rules. Their opposition is based principally upon limitations impacting on their ADP and telecommunications systems, both heavily supported by contractors. Nevertheless, DoD and DIA members support the need for a revised version of DCID 1/7 and have committed to looking anew at the NOCONTRACT rules without waiting until the whole of the DCID is again in need of revision. Thus, as discussed earlier, your approval memoranda carry an acknowledgment of the issue and directs a reexamination. 

3. I believe that we should use this opportunity to break the pattern of modifying the security-related DCIDs by review of the whole of each relevant DCID. A practice of modification of parts of the DCIDs (as is the practice with the Imagery Policy Manual) will allow far more efficient work and should

~~SECRET~~

permit the security rules to be much closer to current than seems to have been past practice. The number of changes required in both 1/19 and 1/7 appear to support this view. The proposed memorandum carrying your approval of this revision sets the stage for this change in procedure.

4. In sum, I recommend that you approve the revision of 1/7 and sign the covering memoranda.



Attachments:
a/s

25X1

25X1

SECRET

[]:CCISCMS/ICS:[]

25X1

Distribution of DCI/ICS-87-0785

- Original - Addressee (w/atts)
- 1 - ADCI (w/atts)
 - 1 - ER (w/atts)
 - 1 - D/ICS (w/atts)
 - 1 - Mark Sullivan, NFI& Secretariat (w/atts)
 - 1 - ICS Registry (w/atts)
 - 1 - CCISCMS Subject (w/atts)
 - 1 - D/CCISCMS Chrono (wo/atts)

ATTACHMENT 12

The Deputy Director of Central Intelligence

Washington, D.C. 20505


DCI/ICS-87-0787

27 February 1987

MEMORANDUM FOR: SCI Forum Members

SUBJECT: DCID 1/7--Approval of Attached Revision

This memorandum records my approval of the attached revision of DCID 1/7 dated 7 January 1984, and directs that work continue to reach an expeditious Community agreement on a final revision of paragraph 8c (NOCONTRACT).


Robert M. Gates
Acting Director

Attachment:
a/s

FOR OFFICIAL USE ONLY

ATTACHMENT 5

The Deputy Director of Central Intelligence

Washington, D.C. 20505

DCI/ICS-87-0786

27 February 1987


MEMORANDUM FOR: NFIB Members

SUBJECT: Revision of DCID 1/7, "Security Controls on the Dissemination of Intelligence Information"

1. This memorandum is to:

- Record my approval of the attached revision of DCID 1/7, "Security Controls on the Dissemination of Intelligence Information."
- Acknowledge that paragraph 8c of DCID 1/7, dealing with the rules embodied in the marking NOCONTRACT, is contentious and is essentially unchanged from language contained in the 7 January 1984 version of 1/7.
- Direct that the SCI Forum report within 90 days on the possibility of better accommodation of the several views of the NOCONTRACT rules.

2. I recognize that the NOCONTRACT rules impact widely throughout the Community, but I charge CIA and DIA to vigorously lead the reexamination of these rules.



Robert M. Gates
Acting Director

Attachment:
a/s

STAT

FOR OFFICIAL USE ONLY



DEFENSE INTELLIGENCE AGENCY
WASHINGTON, D.C. 20301-6111

ATTACHMENT

F

U-6542/OS-4

18 JUN 1986

MEMORANDUM FOR THE CHAIRMAN, DCI SECURITY COMMITTEE

SUBJECT: Revision of DCID 1/7

Reference: DCI SECOM memorandum SECOM-D-135, 9 May 1986, subject as above.

1. By reference, you requested review of the proposed draft revisions to DCID 1/7.
2. DIA wholeheartedly concurs in the decision to issue the revised Directive at the unclassified level. However, DIA does not concur in the remaining revisions. Rather, we believe a reexamination is necessary of both the definition of "NOCONTRACT" information and the controls established for its release.
3. Existing contractor release restrictions are seriously impacting on both current and planned intelligence data handling systems. Because the cost effectiveness of contracting ADP system development and communications has been repeatedly demonstrated, there is virtually no ADP system within the DoD Intelligence Community today that is being built without contractor assistance. As technology keeps abreast of more comprehensive and near real-time collections systems, the requirement for automation of intelligence storage and dissemination will increase. Automated systems require contractor development and support which, in turn, mandates contractor access to data.
4. Two distinct types of contractor access are required and are distinguishable by the deliverables specified in the contract.
 - a. Technical contractors: Deliverables are automated systems to include structured data bases, message handling and associated communications.
 - b. Substantive contractors: Deliverables are intelligence products such as R&D studies, research reports, analytical studies.
5. There are three different types of data involved in contractor release:
 - a. Non-attribution: Finished intelligence products where the source of information is not identified.
 - b. Source-referenced: Finished intelligence with generic source reference (e.g., HUMINT, SIGINT, IMINT) or a source identified (e.g., IR number) but the source itself is not accessible.

c. Raw intelligence: Raw source data included such as in an automated message handling system.

6. DIA believes three actions are required if the policies governing contractor access to intelligence information are to keep pace with the expanding role contractors have within the DoD Intelligence Community.

a. Define contractor access authorized for each contractor and data type combination.

b. Define authority to release intelligence to contractor for each contractor and data type combination.

c. Define required control procedures for data release to contractors for each contractor and data type combination.

7. Based on the foregoing, DIA recommends the following contractor release policy be incorporated into DCID 1/7.

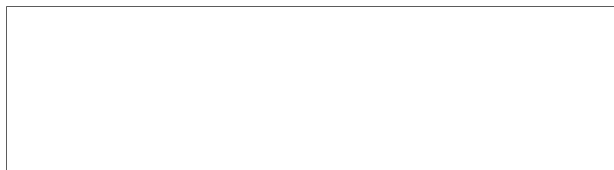
a. Technical contractor access to non-attribution or source referenced data: Release authority is the SOIC. No additional control procedures required.

b. Substantive contractor access to non-attribution intelligence: Release authority is the SOIC. No additional control procedures required.

c. Substantive contractor access to source-referenced intelligence or for both technical and substantive contractor access to raw intelligence: Release authority is the originator of the information. Additional control procedures as specified by the originator.

8. DIA believes that DCID 1/7, as currently structured, is not reflective of the ever increasing and valid requirements for contractor access to intelligence information. Lacking suitable redefinition of "NOCONTRACT" information, DIA is faced with alternatively denying a significant number of requests for data or overwhelming the SECOM with requests for exception to policy.

FOR THE DIRECTOR:



Assistant Deputy Director for
Security and Counterintelligence

STAT

June 1987

OGC-87-51580

ATTACHMENT 6

Policy Statement on Procedures Governing Use of
DCID 1/7 Control Markings

Any authorized recipient of classified intelligence information who desires to use such information in a manner contrary to the control markings authorized by DCID 1/7 (e.g. NOCONTRACT, ORCON, PROPIN, NORFORN) shall obtain the advance permission of the originating agency, as required by paragraph 9 of DCID 1/7. Such a request for permission should be routed through appropriate channels to the Senior Official of the Intelligence Community^{*} (SOIC) with cognizance over the requesting agency, who must be provided sufficient justification along with information describing the nature of the material, its classification, how it will be used, by whom, and the duration for which the permission is requested. The SOIC shall be responsible for seeking advance permission from the originating agency. Once the SOIC has made the request, the originating agency may negotiate with the SOIC or directly with the responsible component of the requesting agency since the originator is the only one who has authority to grant permission to use the information in a manner contrary to the control markings. If a requesting agency desires to use the information in a manner contrary to the control markings for longer than a specified period of time, it should submit a new request at the end of that time, rather than initially requesting permission for an indefinite period of time.

*The SOIC is defined in section 1.7 of Executive Order 12333.

The Director of Central Intelligence

Washington, D.C. 20505

ICS 0790-88

MEMORANDUM FOR: Executive Director
Defense Intelligence Agency

STAT

SUBJECT: Security Policies Governing the Dissemination of
Intelligence Information

REFERENCES: A. Your memo, 22 February 1988 (U-4392/OS-4)
B. DCI Directive 1/7, "Security Controls on the
Dissemination of Intelligence Information,
27 February 1987

1. The concepts and rationale expressed in your 22 February memorandum clearly exhibit the limitations and inhibitions placed on certain DIA operating procedures by strict application of the rules imposed in DCID 1/7. When I approved the revised DCID in February 1987 as Acting Director of Central Intelligence, I understood that there were contentious issues surrounding the NOCONTRACT, as well as other, controls. I realized that the principal objections involved the dissemination caveats as applied to contractors supporting DoD/DIA efforts. I approved the DCID with the understanding that CIA and DIA officers would work together to attempt to resolve the issues, with or without further revision of the DCID. The fact is that CIA and DIA have not continued efforts at negotiating the issues.

2. Your memorandum contains three requests. The first one asks for my support in a joint effort to review existing policy with the objective of establishing new policy to protect sensitive intelligence while permitting Senior Officials of the Intelligence Community (SOICs) to make determinations for release of information as exceptions to the rules. I am disappointed that CIA and DIA have not carried on negotiations over these issues as I directed and expected. I am charging the Community Counterintelligence and Security Countermeasures Office (CCISCMO) of the Intelligence Community Staff (ICS) with responsibility to organize and coordinate meetings between CIA and DIA to discuss and work the issues involved.

SUBJECT: Security Policies Governing the Dissemination of
Intelligence Information

3. The second request asks me to temporarily authorize the SOIC/DIA to permit release of controlled intelligence in DIA data bases where sources cannot be determined. I withhold that permission pending a recommendation from the Director/ICS after he receives a status report following the meetings between CIA and DIA on the overall problem area surrounding the subject. I am requiring such a report and recommendation within 60 days. Should revision of the DCID become necessary, CCISCMO will manage the necessary administrative staffing and Community coordination.

4. With respect to your third request (that DIA be relieved of the requirement for government personnel to be present with SAFE contractors when access to controlled information is possible), this will be a topic for the CIA-DIA negotiators to review since the SAFE program is a joint effort managed by the two agencies. The common element in each of these requests is that particular interests of CIA are involved.

5. Be assured that I am sympathetic to the problems surfaced and the restrictions placed on DIA and, in fact, the entire Community. We share the commitment to the proper dissemination and use of sensitive intelligence information in consonance with our solemn responsibility to protect the sources and methods from which it is produced.

Robert M. Gates
Acting Director

SUBJECT: Security Policies Governing the Dissemination of
Intelligence Information

CCISCMO: [] (3 March 1988)

STAT

Distribution of ICS 0790-88:

Original - [] DIA

STAT

1 - ADCI

1 - ER

1 - AD/ICS

1 - ICS Registry

1 - CCISCMO subject (DCID 1/7)

1 - CCISCMO chrono

1 - [] chrono

STAT